NTIA MULTISTAKEHOLDER PROCESS ON FACIAL RECOGNITION TECHNOLOGY

Risks and Issues Participants Believe Should Be Addressed:
(Following June 3, 2014 Meeting)

(Capitalized terms are as defined by the Definitions group)

1. To what type of entities should each provision of the code appropriately apply: Vendors? Customer-facing entities? Operators of cameras (such as private shopping malls)? Operators of security systems? Photojournalists? Amateur photographers? Operators of other camera-enabled devices? End users of the facial recognition data?

2. *Issue: What obligations should the code impose when Facial Detection occurs but no Facial Template is created and no individual is enrolled?*

    a. In Facial Detection, where a face is detected ("this is a human face") but no Facial Template is created, is transparency and consent possible?

    b. If so, what transparency would be required and how would it be implemented?

    c. Is it appropriate to requires consent? How could this be implemented?

3. *Issue: What obligations should apply when a Facial Template is created and but is <u>not</u> enrolled (stored)?*

    a. Should transparency be required and how would it be implemented?

    b. Is it appropriate to requires consent? How could this be implemented?

4. *Issue: What obligations should apply when a Facial Template is created and is enrolled (stored); Risk: individuals could be enrolled in commercial facial recognition databases without their knowledge; or without their consent.*

    How should the code address transparency and informed consent at the time a Facial Template is enrolled?

    a. How should the concepts of transparency and consent apply to the use of the technology for Authentication (*e.g.*, passports, employee ids; device access; ATM cards)? Is it reasonable to presume consent from a Subject's enrollment if the purpose has first been explained?

    b. How should transparency and consent to enrollment be implemented in contexts where the technology will be used for purposes other than Authentication?

c. In scenarios in which a face is matched with a Facial Template, but there is no associated identification metadata (*e.g.*, "this face has been here before" but no identification), is transparency and consent possible and, if so, how would they be implemented?

d. In scenarios in which identification information is attached to a Facial Template, is transparency and consent desirable and, if so, how would they be implemented?

e. Should the code's requirements for transparency and consent differ between (a), (b), (c), and (d) and, if so, how?

f. What are the best ways to ensure individuals have meaningful control over when and how a Facial Template is enrolled, and how derivative data are used?

5. *Risk: A code of conduct could preclude or hinder meritorious uses of commercial facial recognition technology*.

a. Should the potential of the software to promote safety and security, deter crime, enhance consumer experiences, or drive technological innovation be facilitated by the code and, if so, how? What other benefits should be facilitated by the code in the areas of health, education, empowering individuals with disabilities, and many others?

b. Would a narrow, prescriptive code hinder other future uses of facial recognition technology? Would a set of best practices better promote responsible uses of facial recognition technology without circumscribing uses that will be socially and economically beneficial?

6. *Risk: Individuals could be denied products or services unless they consent to enrollment of a Facial Template*.

Should the code address the availability of alternative means for achieving the intended purpose of a particular use of the software that do not involve a Facial Template? In other words, are there instances in which enrollment is mandatory, or should the code address whether individuals should have options? What is the range of contexts in which such options should become available, and what factors should be considered? Are there scenarios in which this is infeasible or not possible and, if so, how do these fit into the code?

7. *Risk: Commercial use of facial recognition technology could infringe on individuals' autonomy (including right to travel) and erode personal privacy (including right to be let alone and right to publicity) by allowing for collection of additional data points.*

    a. How should the concept of personal autonomy be addressed by the code? Is it a separate consideration, or is it better addressed within the context of other issues? What sort of consent is appropriate? Are there concrete examples of how personal autonomy has been, or plausibly would be, infringed by commercial use of facial recognition?

    b. Should the code address implications of the technology on common law rights of publicity?

    c. How would the use of facial recognition technology meaningfully impact the common law right of publicity in a way that "manual" detection or recognition of photos would not?

8. *Risk: Commercial use of facial recognition technology could, as a practical matter, reduce individuals' anonymity in public and chill rights of free speech, free press, and free assembly.*

    a. Should, and if so how, the code address anonymity in public? What are real world examples of how facial recognition technology has or is likely to reduce individuals' anonymity in public? (In the example of a face being recognized in a demonstration, presumably the face could be identified through facial recognition only if the person's image was already in a database to which the photographer also had access, or if other circumstances existed that would enable the photographer to identify the person.)

    b. Would a broadly-drafted code risk circumscribing journalists' ability to report on public events or identify participants in those events? How does the concept of transparency apply in this scenario? Should this be regarded as a form of secondary use or downstream use (is there a difference between secondary and downstream uses)?

    c. Should the code separately address the possibility that facial recognition technology could enable someone to be identified and stalked or harassed by a stranger?

9. *Risk: Commercial use of facial recognition could enable entities to develop profiles by merging personal data collected online from individuals and their personal networks with individuals' activities offline without individuals' knowledge or consent; Commercial use of facial recognition could result in secondary or downstream uses of personal data in ways that consumers do not understand and did not anticipate*.

How should the code implement the principles of transparency, control, and respect for context in connection with secondary or downstream uses and sharing?

   a. Should the code contain a definition of a secondary or downstream use and, if so, what would that be?

   b. What, if any, secondary or downstream uses of Facial Detection ("this is a human face") should be addressed?

   c. What, if any, secondary or downstream uses of facial recognition ("this face has been here before") should be addressed?

   d. What, if any, secondary or downstream uses of Facial Identification ("this face sufficiently matches a specific Facial Template") should be addressed?

   e. What, if any, secondary or downstream uses of Facial Profiling ("this face is a specific gender/race/age") should be addressed?

   f. What is the harm from each type of secondary or downstream use that the code might address?

   g. Should the code address whether consumers may be required to consent to secondary or downstream uses in order to use the primary product or service?

   h. Should the code address implications of the technology on common law rights of publicity?

10. *Risk: Commercial use of facial recognition technology could result in discriminatory practices or patterns of behavior.*

Should, and if so how, the code address uses of facial recognition technology, which may collect sensitive data categories, that result in discriminatory practices (such as price discrimination) or patterns of behavior, such as predatory marketing or unwanted solicitations? What concrete risks or harms would the use of facial recognition technology pose that would not otherwise be posed through the use of other technologies or methods?

11. *How should the code address storage of Facial Templates?*

    a. Should the code address retention periods? Should retention periods depend on the individual's reasonable expectations regarding use and retention of the template?

    b. Should the code define Secure Storage of Information? Should context matter and, if so, how?

12. *Risk: Commercial facial recognition data could be subject to data breaches that result in sensitive biometrics being revealed to unauthorized entities; insufficient security procedures could result in biometric identity theft.*

    a. What entities would be best situated to provide for security?

    b. What data should be subject to security obligations in the code?

    c. Most states currently have breach notification laws. Should the code impose additional data breach notification obligations (not otherwise subject to state law)?

    d. Are there contexts in which the code should require encryption of Facial Recognition Data?

    e. Should the code distinguish between unencrypted Facial Templates and those that are encrypted? Could the code do so by establishing a "material risk of harm" threshold for notice, where a "material risk of harm" would arise when unencrypted templates are revealed to unauthorized entities? Would treating encrypted templates as not triggering a material risk of harm provide companies with appropriate incentives to design and implement robust security protections?

13. *Risk: Commercial facial recognition technology could increase privacy and security risks for teens. What is the best way to account for a teen's age and level of understanding in developing a code and consent framework?*

    a. Should, and if so how, the code address the use of the technology when the individuals whose faces are being scanned are 13 to 18 years old? How would age be known? Should the code apply only when a Facial Template is created?

    b. Facial recognition technology may increase the risk that teens may be subjected to predatory marketing or permanent profiling (*e.g.*, for education, school admissions, credit, housing, employment, insurance, etc.) To what concrete risks or harms would minors be subjected through the use of facial recognition technology that they would not otherwise be subject to through other technologies or methods?

c. How should the code account for imprecision in facial recognition technology's ability to distinguish ages (*e.g.*, the technology may have trouble distinguishing between an 18 year old and a 16 year old, or between a 13 year old and a 12 year old). Should the code establish separate requirements or presumptions for companies whose primary audience is teens? Should companies determine age when a Facial Template is created, or when a Facial Template is linked to an identifier? Is there a way to make age determination without collecting more information?

14. *Risk/Issue: Children under 13*.

How should the code best apply to faces of children under 13? How can the code best protect children under 13? How should the code accommodate parents' interest and right to have a say in any data collection about their children? Should the code restrict the use of Facial Templates of children under the age of 13 to security/authentication purposes? Should the code restrict the use of the technology in areas in which there are large numbers of kids or the target audience is kids? Should parental consent waive broad restrictions on the use of facial recognition technology for children under 13? Should the code impose COPPA-type requirements and, if so, how could parental consent be obtained?

a. Should, and if so how, the code address commercial uses of facial recognition technology that are subject to the Children's Online Privacy Protection Act?

b. What commercial uses of facial recognition technology, as applied to children under 13, fall outside the scope of COPPA?

b. Should, and if so how, the code address commercial uses of facial recognition technology that are not subject to the Children's Online Privacy Protection Act?

15. *Risk: Individuals could be denied access to products or services based on erroneous identifying information derived from commercial facial recognition*.

Should, and if so how, the code address how individuals might seek correction in the case of false negatives or false positives? What would be reasonable means for individuals to seek correction from commercial entities? What entities should be responsible for handling these matters? Should the purpose for which the technology is being used be a factor?

16. *Risk/Issue: Withdrawal of Facial Template from a database?*

a. Is there a difference between withdrawal from a database and deletion from a database?

b. Should the code address withdrawal/deletion from the database? If so, how can organizations best provide individuals with the ability to withdraw or request deletion from enrollment in facial recognition databases? Is there anything to be withdrawn other than a Facial Template?

c. Should the code address withdrawal/deletion in situations where the individual maintains an ongoing commercial relationship with the User?

d. Are there contexts in which the User need not allow a person to withdraw or request deletion?

e. How would withdrawal/deletion of a Facial Template from a database compare with withdrawal/deletion of other personal data?

17. *Risk: The code of conduct might fail to prioritize the worst harms that could arise from the commercial use of facial recognition technology, or might fail to address any concrete harm posed by facial recognition technology*.

How can the code focus on finding effective solutions that address the most egregious harms and pose the greatest risks to individuals, where these harms are not already addressed by existing laws?

18. What should the code say about government (*e.g.*, law enforcement) access to raw images, Facial Templates, or algorithms obtained by the commercial sector? What standards should apply to requests by governments to gain access to this information, and what concrete risks would occur if this standard is set too low or too high?